DIVISION ALGORITHM

Theorem 1.1: Let $a, b \in \mathbb{Z}$ with the condition that $b > 0$, then there exist unique q and r which satisfies

$$a = qb + r \qquad (0 \leq r < b)$$

where: $q \rightarrow$ the quotient

$r \rightarrow$ the remainder when a/b (a is divided by b)

Proof: We need to show that:

(i) set S is nonnegative and is nonempty such that $S = \{a - xb |\ x \in \mathbb{Z}\,; a - xb \geq 0\}$

where S is the set of integers k such that $0 \leq k < b$;

(ii) Set S contains smallest integer r (remainder when a/b) ; and

(iii) The uniqueness of integers q and r.

Proof: We consider the set $S = \{a - xb | x \in \mathbb{Z}\,; a - xb \ \geq 0\}$

i. ***Need to Show*****:** The given set S is nonnegative and nonempty.

Since $a - xb \geq 0$, therefore $a - xb$ is nonnegative. Also, integer $b \geq 1$ and let $x = -\,|a|$ for x can be a negative or positive integer.

So, we have:

$$\begin{aligned} & a - xb \geq a + |a| \ \geq 0 \\ \Rightarrow\ & a - (-|a|)\, b \geq a + |a| \geq 0 \\ \Rightarrow\ & a + |a|\, b \geq a + |a| \geq 0 \end{aligned}$$

Thus, for $x = -\,|a|$, $a - xb$ lies in set S and is nonempty.

ii. ***Need to Show*****:** By the definition of Well-being Principle that S contains smallest integer r.

Let r be the smallest integer in . Then from the given equation of Division Algorithm, we have:

$$a = qb + r$$

$$\Rightarrow \ a + -qb = qb + r + -qb$$

$$\Rightarrow \ a - qb = r$$

And since r is the smallest integer, let $r < b,$ that if contradicted, then $r \geq b$, then we have:

$$r = a - qb \geq 0$$
$$\Rightarrow r + -b = a - qb + -b \geq 0$$
$$\Rightarrow r - b = a - (qb + b) \geq 0$$
$$\Rightarrow r - b = a - (q + 1)\, b \geq 0$$

Observe that $a - (q + 1)\, b = r - b < r.$ Then by contradiction, r is the smallest element of set S since $r - b \geq 0$ and $r - b \in S$ but $r - b < r.$ Thus, $r < b$.

iii. Need to Show: The uniqueness of integers q and r.

Suppose we have:

$$a = qb + r = q'b + r'$$

where:

$$0 \leq r < b$$

$$0 \leq r' < b$$

So that:

$$qb + r = q'b + r'$$

$\Rightarrow \ qb + r + -\, q'b = +\, r' + \, -\, q'b$ ***Adding $-\, q'b$ on both sides***

$\Rightarrow \ qb + (r + \, -\, q'b) = \ q'b + (\, r' + \, -\, q'b)$ ***Associative Property of Addition***

$\Rightarrow \ qb + (-\, q'b + r) = \ q'b + (-\, q'b + r'\,)$ ***Commutative Property of Addition***

$\Rightarrow \ (qb + \, -q'b) + r = \ (q'b + -\, q'b) + r'$ ***Associative Property of Addition***

$\Rightarrow \ (qb + \, -q'b) + r = 0 + \ r'$ ***RHS: Simplifying*** $(\boldsymbol{q'b} + -\, \boldsymbol{q'b})$

$\Rightarrow\ (qb - q'b) + r = r'$ ***LHS: Definition of Subtraction***

RHS: Identify Property of Addition

$\Rightarrow\ (qb - q'b) + r - r' = r' + -r$ ***Adding -r to both sides***

$\Rightarrow\ (qb - q'b) + 0 = r' + -r$ ***LHS: Simplifying*** $\boldsymbol{r + -r}$

$\Rightarrow\ (qb - q'b)\ = r' - r$ ***LHS: Identity Property of Addition***

RHS: Definition of Subtraction

$\Rightarrow\ b(q - q')\ = r' - r$ ***LHS: Factor out b from*** $\boldsymbol{(qb - q'b)}$

Rewriting this with the fact that absolute value of a product is equal to the product of the absolute value, then:

$$b\ (q - q') = r' - r$$

$$\Rightarrow\ \ |b|(q - q') = |r' - r|$$

$$\Rightarrow\ \ b|q - q'| = |r' - r|$$

It follows that $0 \leq |r' - r| < b$ which yields $0 \leq b|q - q'| < b$.

Then we have:

$(0\ \leq b\ |q - q'| < b)\ 1/b$ ***Multiply*** $\boldsymbol{1/b}$ ***to all sides of the inequality***

$$\frac{0}{b} \leq \frac{b|q-q'|}{b} < \frac{b}{b}$$

$\Rightarrow\ (0\ \leq |q - q'| < 1)$ ***Which we get*** $\boldsymbol{|q - q'| = 0}$ ***for*** $\boldsymbol{|q - q'|}$ ***is nonnegative.***

Thus, $\boldsymbol{q = q'}$ ***and*** $\boldsymbol{r = r'}$***.***

Corollary to Theorem 1.1: If a and b are integers with $b \neq 0$, then there exist unique integers q and r such that

$$a = qb + r \qquad , \qquad (0 \leq r < |b|)$$

Proof: Notice that $|b| > 0$ whether b is negative or positive by definition of absolute value of any integer b.

It follows from Theorem 2.1 that for $|b| > 0$, there exist integers q' and r such that:

$$a = qb + r \qquad , \qquad (0 \leq r < b)$$

$$a = q'|b| + r \qquad , \qquad (0 \le r < |b|)$$

To illustrate Division Algorithm when $b < 0$, we take for instance $b = -7 < 0$, then for values of $a = 1, -2, 61$ and -59.

We have:

$$a = qb + r$$

$$\left.\begin{aligned} 1 &= 0\,(-7) + 1 \\ -2 &= 1\,(-7) + 3 \\ 61 &= (-8)(-7) + 5 \\ -59 &= (9)(-7) + 4 \end{aligned}\right\} \quad \boxed{\begin{array}{l}\text{The values of } r \text{ are} \\ r < |b| = |-7| \end{array}}$$

And for instance with $b = 2$, the possible remainders are $0 \le r < b = 2$ that is:

i. If $r = 0$, $a = 2q$ $\rightarrow$ even form

ii. If $r = 1$, $a = 2q + 1$ $\rightarrow$ odd form

If we have a^2, then its either:

i. $(2q^2) = 4q^2 = 4k \quad , \quad (k = q^2 \in \mathbb{Z})$

ii. $(2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4k + 1 \quad , \quad (k = q^2 + q \in \mathbb{Z})$

Where the square of an integer leaves the values of $r = 0, 1$ upon division b 4.

Another illustration is that the square of any odd integer can be written in the form $8k + 1$. By Division Algorithm, any integer is representable as one of the forms: $4q$, $4q + 1, 4q + 2$ and $4q + 3$.

Example 1: Odd integers 9 and 11. Squaring these integers,

we have:

i. $9^2 = 81 = 8(10) + 1 \quad , \quad (k = 10)$

ii. $11^2 = 121 = 8(15) + 1 \quad , \quad (k = 15)$

Example 2: We are needed to show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \ge 1$.

Solution: By Division Algorithm either $a = 3q, 3q + 1$, or $3q + 2, q \in \mathbb{Z}$.

i. ***First case:*** When $a = 3q$

$$\frac{a(a^2+2)}{3} = \frac{3q[(3q)^2+2]}{3} = q(9q^2+2) = 9q^3 + 2q$$

Since 2, 9, q ∈ ℤ, then $9.q.q.q = 9q^3, 2.q = 2q \in \mathbb{Z}$ by ***Closure Property for Multiplication***.

Also, since $9q^3, 2q \in \mathbb{Z}$, then $9q^3 + 2q \in \mathbb{Z}$ by ***Closure Property for Addition.***

Thus, $\boldsymbol{9q^3, + 2q}$ ***is an integer.***

ii. ***Second case:*** *When* $a = 3q + 1$

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)[(3q+1)^2+2]}{3} = \frac{(3q+1)(9q^2+6q+1+2)}{3}$$

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)(9q^2+6q+3)}{3}$$

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)\,.3\,(3q^2+2q+1)}{3}$$

$$\frac{a(a^2+2)}{3} = (3q+1)(3q^2+2q+1)$$

Since $2, 3, \mathrm{q}, \in \mathbb{Z}$, then $2\mathrm{q}, 3.\mathrm{q}.\mathrm{q} = 3\mathrm{q}^3 \in \mathbb{Z}$ by ***Closure Property for Multiplication***.

Also, since $1, 2q, 3q, 3q^2 \in \mathbb{Z}$, then $3q + 1,\ 3q^2 + 2q + 1 \in \mathbb{Z}$ by ***Closure Property for Addition.***

Thus, $(\boldsymbol{3q+1})\ (\boldsymbol{3q^2+2q+1})$ ***is an integer by Closure Property for Multiplication.***

iii. ***Third case:*** When $\mathrm{a} = 3\mathrm{q} + 2$

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)[(3q+2)^2+2]}{3} = \frac{(3q+2)(9q^2+12q+4+2)}{3}$$

$$\frac{a(a^2+2)}{3} = \frac{(3q+2)(9q^2+12q+6)}{3}$$

$$\frac{a(a^2+2)}{3} = \frac{(3q+2)\,.3\,(9q^2+4q+6)}{3}$$

$$\frac{a(a^2+2)}{3} = (3q+2)(3q^2+4q+2)$$

Since $3, 4, \mathrm{q} \in \mathbb{Z}$, then $3\mathrm{q}, 4\mathrm{q}, 3.\mathrm{q}.\mathrm{q} = 3\mathrm{q}^2 \in \mathbb{Z}$ by ***Closure Property for Multiplication.***

Also, since $2, 3q, 4q, 3q^2 \in \mathbb{Z}$, then $3q + 2, 3q^2 + 4q + 2 \in \mathbb{Z}$ by ***Closure Property for Addition.***

Thus, $(\boldsymbol{3q+2})\ (\boldsymbol{3q^2+4q+2})$ ***is an integer by Closure Property for Multiplication.***